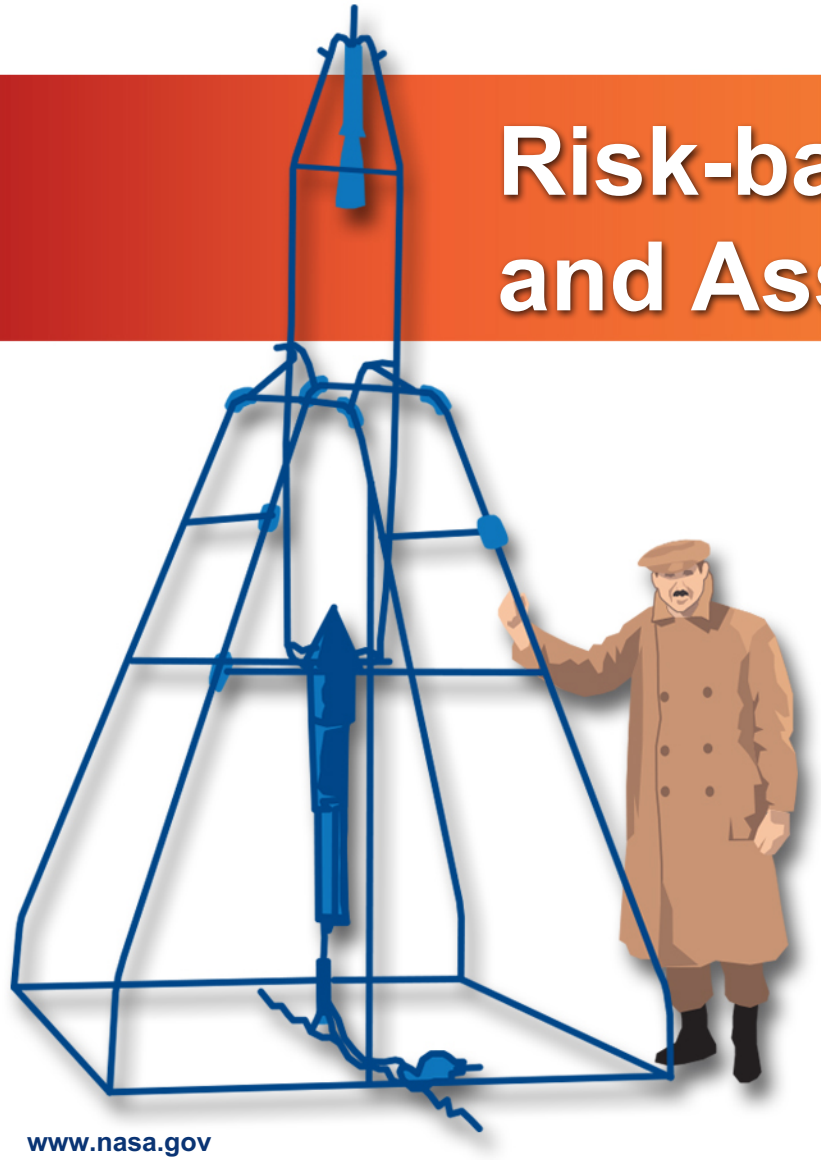
National Aeronautics and Space Administration

Risk-based SMA: Audit and Assessment



GSFC Safety and Mission Assurance

Jesse Leitner, Chief Engineer

SAFETY and MISSION ASSURANCE DIRECTORATE Code 300

SMA SAFETY and MISSION ASSURANCE NASA Goddard

Agenda

- Risk Classification and Risk-based SMA
- Day in the life
- Risk-based implementation of ISO 9001
- Risk-based SMA Examples and current activities
- PCB example

National Aeronautics and Space Administration

GPR 8705.4: Risk Classification and Risk-based SMA

SAFETY and MISSION ASSURANCE 3
DIRECTORATE Code 300

SMA
SAFETY and MISSION ASSURANCE
NASA Goddard

www.nasa.gov

GPR 8705.4

- GSFC implementation of NPR 8705.4
- Establishes Risk-based SMA as GSFC policy
- Risk Classification Definitions
- Nonconformance handling
  - Do not reject without understanding the risk
  - Determine cause of NC before reproducing the item (even from different vendor)
- Guidelines for activities vs mission class
- Formalizes sub-Class-D risk postures
- Ultimately will be one element used to develop project Mission Assurance Requirements vs mission class
  - How does a project demonstrate that they are developing a Class “X” product?
  - How do we convey to a vendor what we expect for Class “X”?

Mission Success Activities vs. Risk Posture

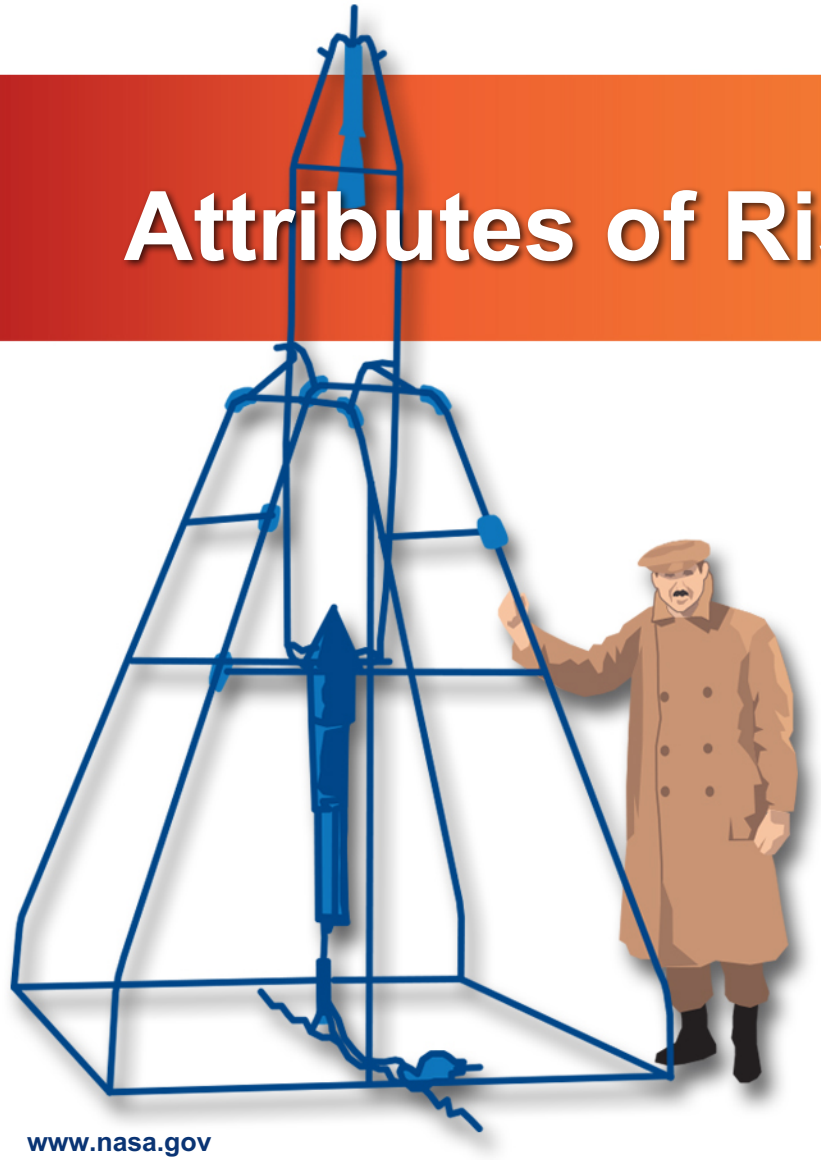
(example elements)

Technical Categories	Class A	Class B	Class C	Class D	Ground System (GS)	7120.8 Class	Do No Harm (DNH)	Hosted Payload Class (host requirements)
Single point failures (SPF)	Any SPF against Level 1 requirements necessitates a specific waiver, SPF analysis expected per GPR 7123.1	Particular attention to avoidance, tracking, and mitigation, SPF analysis expected per GPR 7123.1. Highly fault-tolerant, through redundancy and other means.	Selective redundancy for tall pole items, tracking, and communication, tall pole, critical item, or SPF analysis	SPF, critical item, or tall pole analysis up front, communication of results. Selective redundancy where cost effective.	N/A	Project best effort. Tracked in project documen-tation.	Project best effort	NASA review of design history
EEE Parts	Level 1 parts per EEE-INST-002; DPA performed per S-311-M-70; Counterfeit Avoidance requirements per 500-PG-4520. 2.1;	Level 2 parts per EEE-INST-002 except Level 1 parts for single point failures and hybrids containing active components; DPA performed per S-311-M-70; Counterfeit Avoidance	Level 2 parts per EEE-INST-002 for missions greater than 2 years except Level 1 parts for hybrids containing active components and Level 3 parts may be used for fault tolerant, non-critical	Level 3 parts per EEE-INST-002 except Level 2 parts for hybrids containing active components; DPA performed per S-311-M-70; Counterfeit Avoidance requirements	For custom designed module, quality level of parts selected needs to be consistent with the criticality of the module.	Best commer-cial practices, advise on part selection & derating. ISO certified facilities preferred.	Best commer-cial practices, ISO certified facilities preferred.	Host practices. Advise on part selection & derating.

**Excerpt from GPR 8705.4*

National Aeronautics and Space Administration

Attributes of Risk-based SMA



SAFETY and MISSION ASSURANCE 6
DIRECTORATE Code 300

SMA
SAFETY and MISSION ASSURANCE
NASA Goddard

www.nasa.gov

What is Risk-Based SMA?

The process of applying limited resources to maximize the chance for safety & mission success by focusing on mitigating specific risks that are applicable to the project vs. simply enforcing a set of requirements because they have always worked

Risk-based SMA

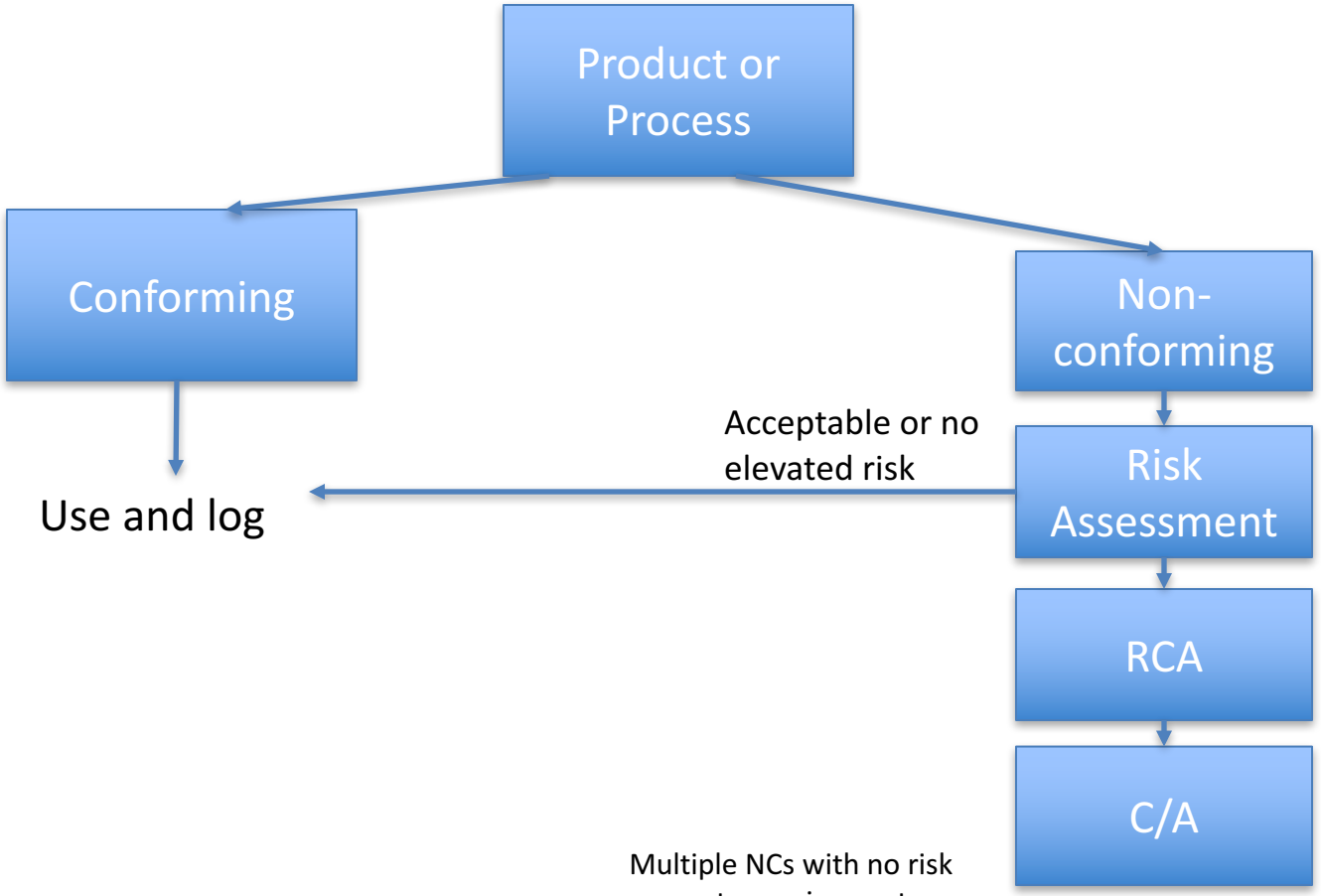
- Risk-informed framework
- Risk-informed requirements generation
- Risk-informed decisions
- Risk-informed review and audit

Attributes of Risk-Based SMA

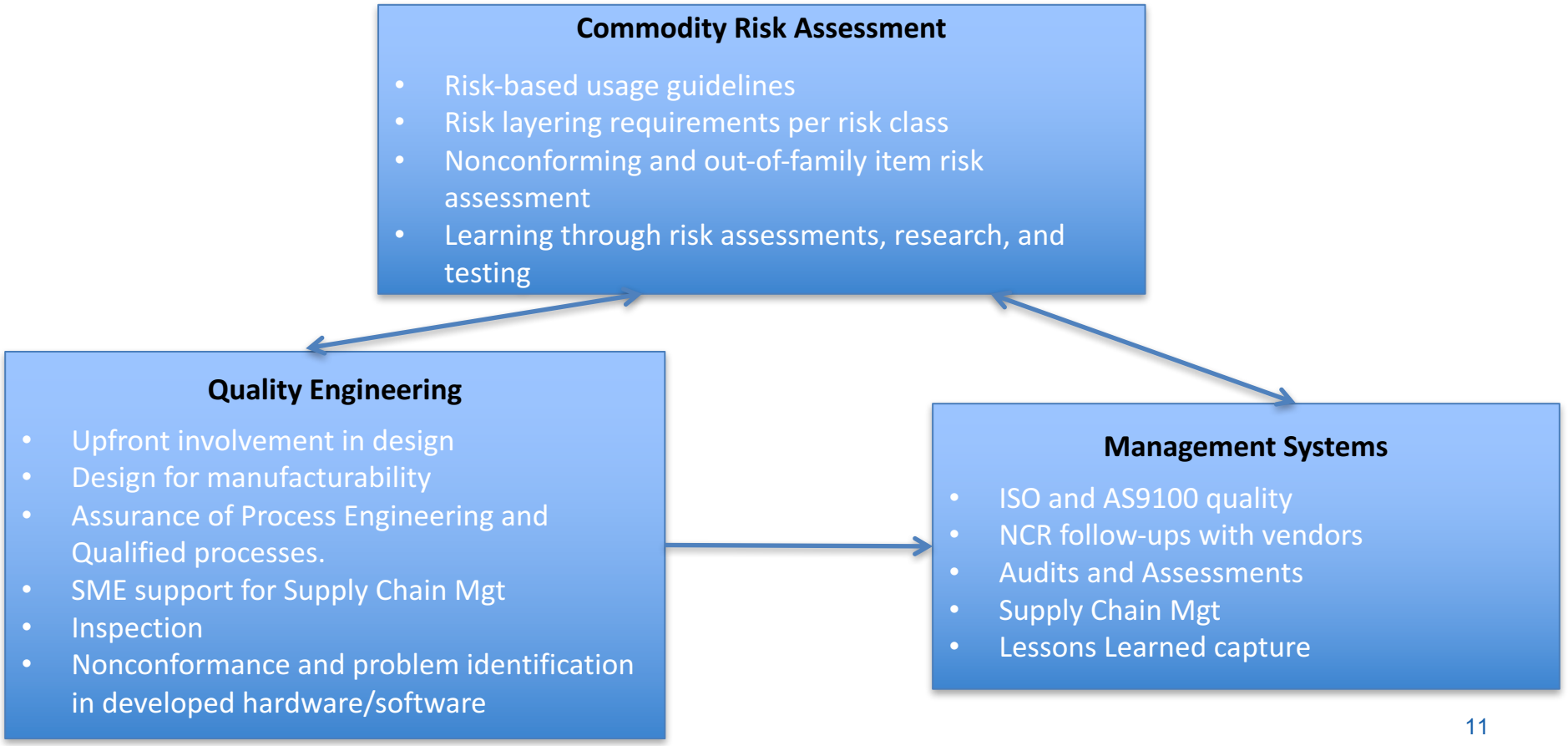
- *Upfront assessment* of reliability and risk, e.g. tall poles, to prioritize how resources and requirements will be applied
- *Early discussions* with developer on their approach for ensuring mission success and responsiveness to feedback
- *Judicious application* of requirements based on learning from previous projects and the results from the reliability/risk assessment, and the operating environment (Lessons Learned – multiple sources, Cross-cutting risk assessments etc)
- *Characterization of risk* for nonconforming items to determine suitability for use – project makes determination whether to accept, not accept, or mitigate risks based on consideration of all risks
- *Continuous review* of requirements for suitability based on current processes, technologies, and recent experiences
- *Consideration* of the risk of implementing a requirement and the risk of not implementing the requirement.

Note: Always determine the cause before making repeated attempts to produce a product after failures or nonconformances

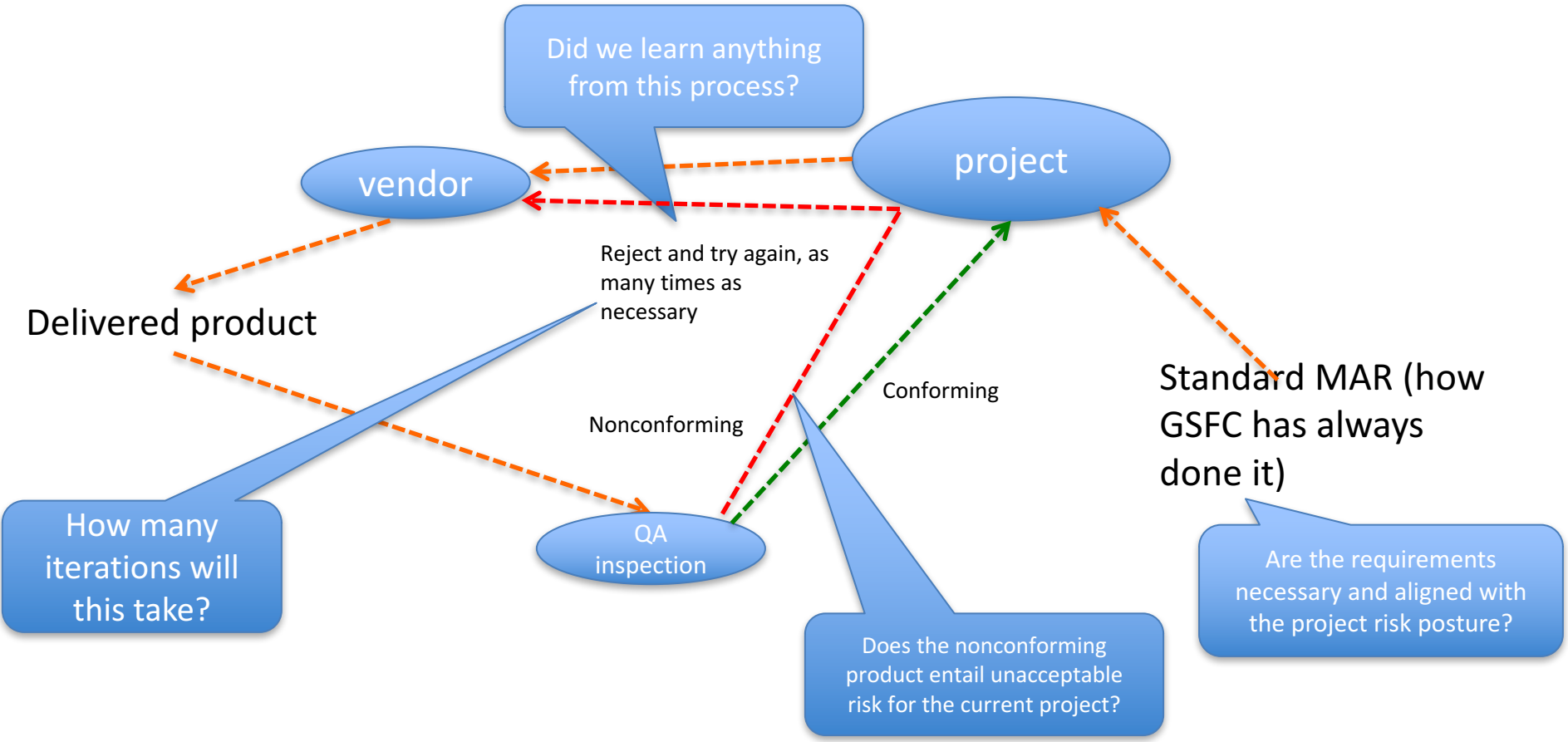
Big Picture of Risk-based SMA



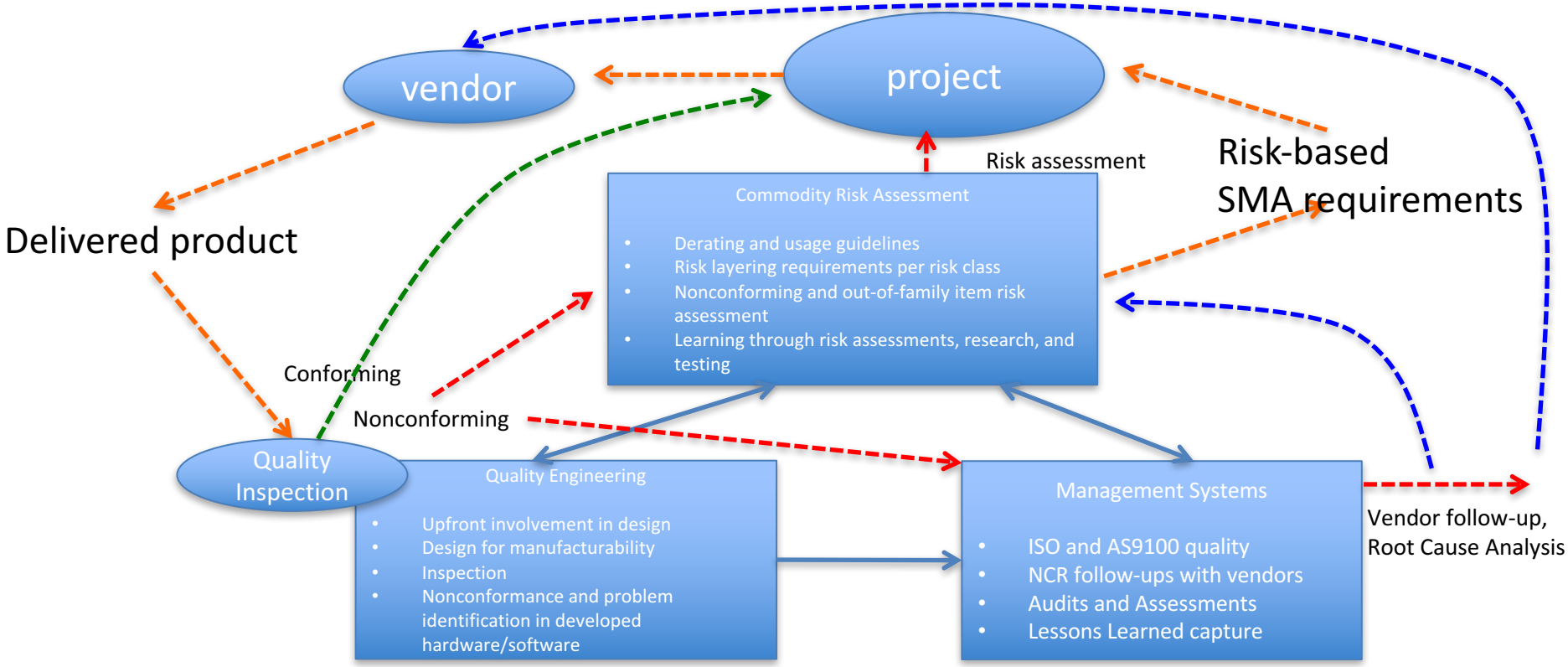
The GSFC Quality Triangle



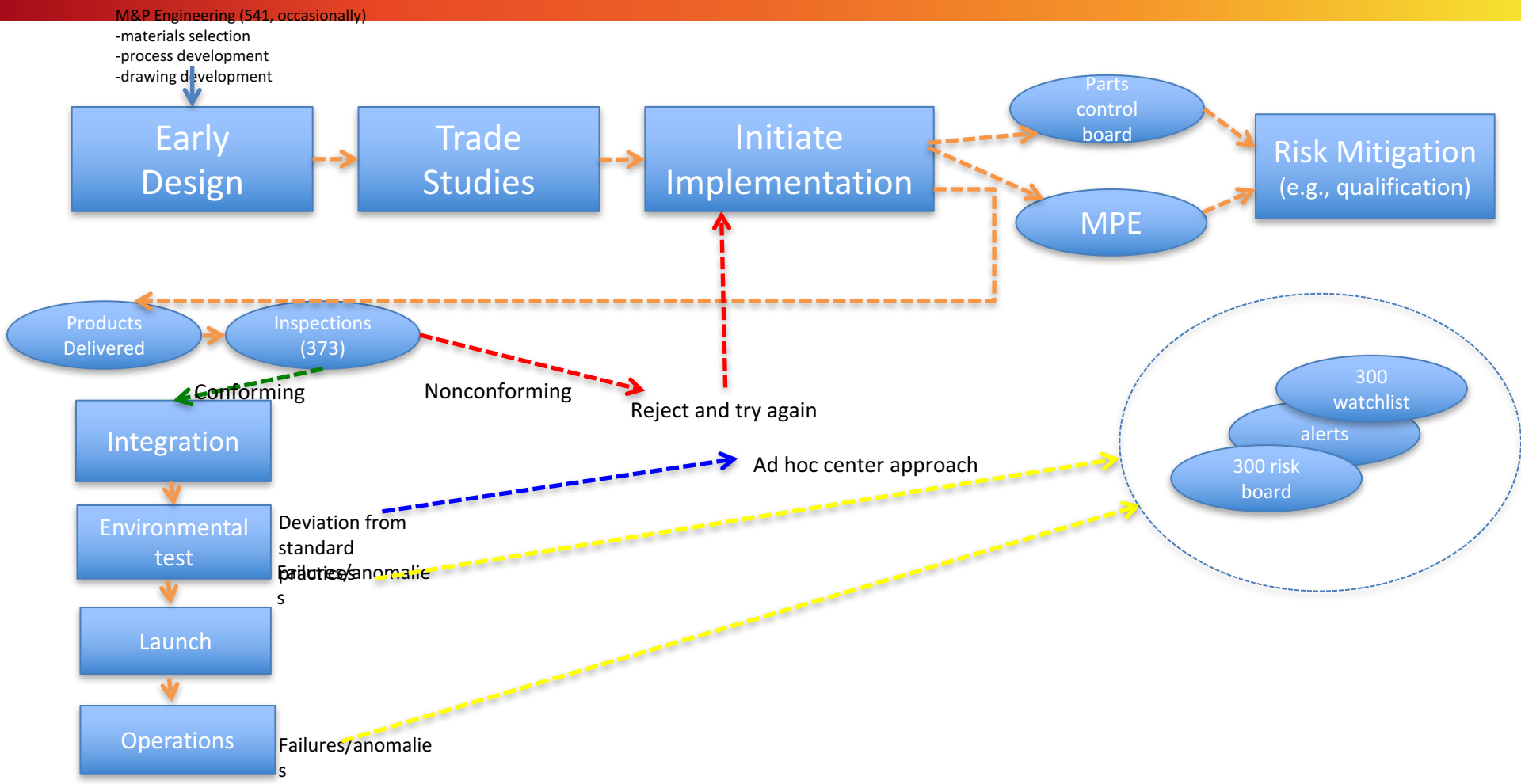
Day in the life example - yesterday



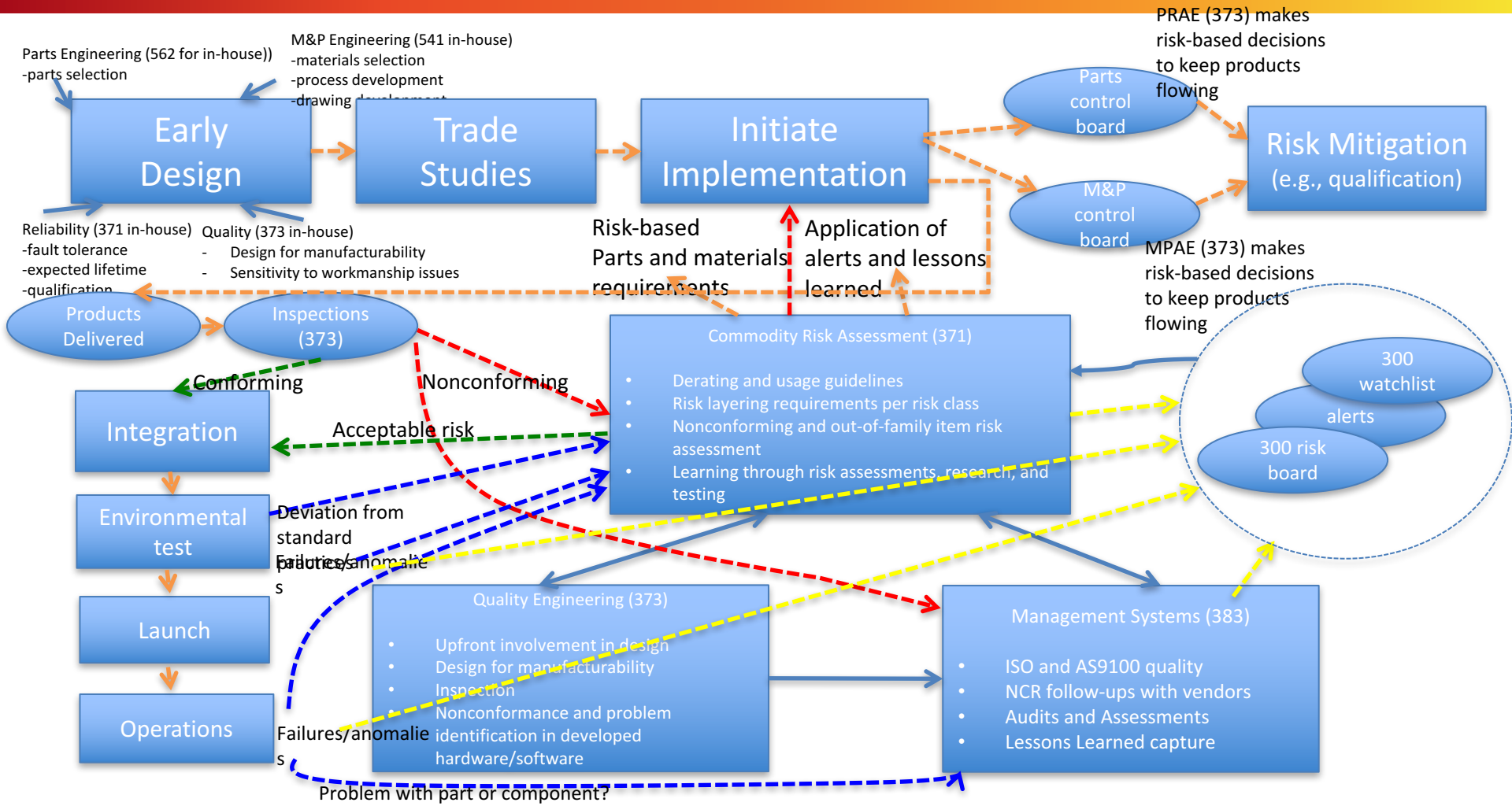
New day in the life - generic product delivery example



Design & Implementation (yesterday)



Design and Implementation



National Aeronautics and Space Administration

Risk-based ISO implementation

SAFETY and MISSION ASSURANCE DIRECTORATE Code 300

SMA SAFETY and MISSION ASSURANCE NASA Goddard

New features in 2015

- Document organization: written under “High Level Structure”
- Risk management is at the core
- Commitment to quality through strong leadership is strengthened
- Better consideration to how organizations evolve to improve
- The role of the quality manual is reduced – focus is more on keeping up with technological and societal changes
- More emphasis given to the context surrounding the organization
- Knowledge is now a resource to manage

Focus is on risk and lessons learned/knowledge acquisition

Perform risk-based audit and assessment

- Assessors document nonconformances to requirements and observations of nonstandard practices
- Make first cut at determining whether credible risk is present due to NCs and observations, or if other areas of risk are identified
- Identify findings accordingly to the developer and affected projects
- Project and SMA organization assess risk associated with each finding
  - in some cases, RCA is required to determine if there is a systemic problem
- Those that involve elevated risk will prompt RCCA
- Common findings across multiple developers with no elevated risk indicates that there is a requirements problem
  - In this case, we move to fix the requirement

Look for risks: Pre-2015 vs risk-based

Pre-2015	Risk-based
Met-cal: check stickers on all "boxes" in a room	Inquire about which measurements have documented accuracy requirements. Check cal status of instruments used to take those measurements
ESD: Lack of ESD controls based on finding in high-risk area	Determine controls on high-risk area (beyond simply ESD) to find out if there is a clear distinction between where risks can be taken and where they can't
Use of materials beyond date (or no date)	Assess organization's understanding about expiration of materials and risks associated beyond the date
Use of standards other than those specified	Determine whether org understands the standard they use and whether they properly negotiate requirements with customer
Not meeting sampling rate requirements	Determine whether org makes "quality adjustments" to sampling

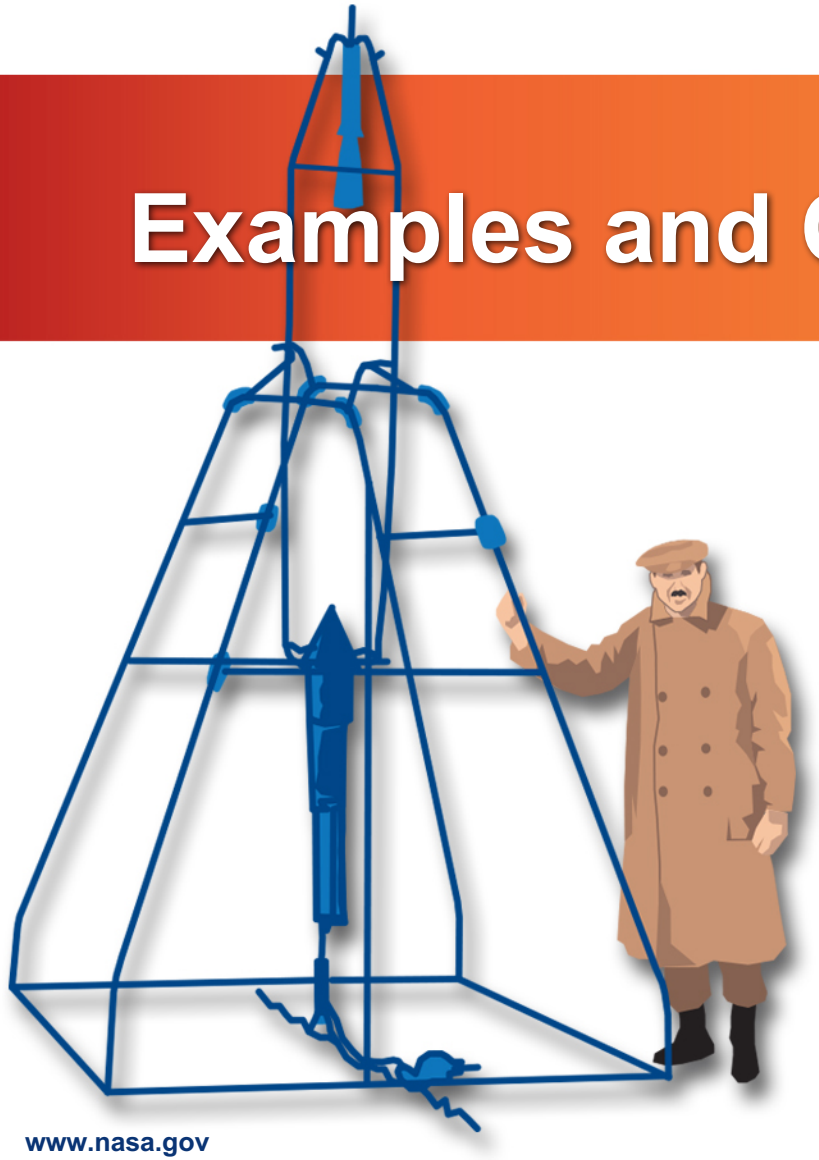
Setting a path for risk-based ISO

- Establish risk-based engineering and SMA policy (GPR 8705.4)
- Maintain a rigorous risk management process (GPR 7120.4)
- Develop and maintain has a well-defined structure, both in organization and process, to support risk-based decisions
- Use risk as a basis to establish process changes based on audit and assessment findings (e.g., metrology/calibration)
- While many in industry are risk-driven in their process definitions and responses to audits, go beyond that by using a rigorous and well-documented process
- Create positions in the organization centered on risk and learning, day-to-day

Positions Centered on Risk and Learning

- Risk
  - **Ensure that proactive and reactive actions are informed by risk in proper context of the project**
  - Operating at the lowest risk posture supersedes simply meeting lower level requirements
- Learning
  - **Ensure that lessons at all levels are applied from project to project and that subsequent assessments continuously improve in efficiency and effectiveness.**
  - Lessons learned are among everyone's job, but these positions are the leaders in applying the lessons learned in everyday activities.
  - Lessons learned are implemented in daily practices for continuous improvement

Examples and Current Efforts



Risk-based SMA Examples

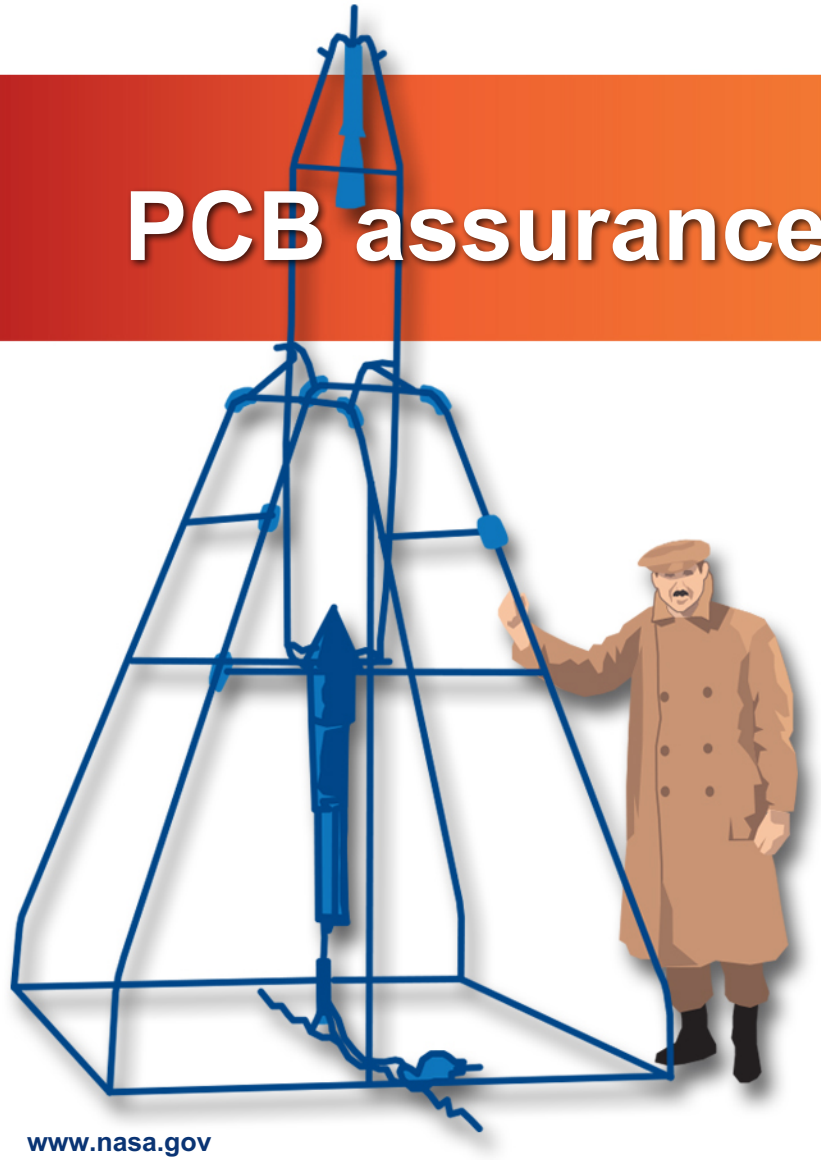
- Printed circuit board coupon NC process
  - Over 140 panels would have been rejected by previous process with no elevated risk (hundreds of weeks, $Ms)
- PCB bromine restriction
  - Requirement prompted vendors to change working processes, great increases in cracking, crazing, and wicking
- PCB copper wrap requirement
  - Requirement for blind and buried vias, costly and difficult to meet, testing proves no reliability improvement
- GOES-R transistors
  - Overly conservative failure prediction of moisture alone prompts much riskier rework in fully tested system
- DC/DC converters
  - Warnings about “top two” converters drive projects to much lower quality devices
- ELC reverse capacitors
  - Assessment did not properly consider moisture effects
- Semicoa GIDEP
  - Low incidence concern leads to high risk rework

Current Efforts

- Correlation of parts failure rates (ground and on-orbit) against screening levels (1, 2, 3)
  - Requirements should be commensurate with actual experiences
- Characterization of reverse tantalum capacitors
  - Moisture and temperature effects
- PCB reliability vs selected standard (IPC 6012, Class 2, Class 3, Class 3/A, MIL-55110)
  - Copper wrap testing complete, paper being finalized
  - Internal annular ring testing has commenced
  - Etchback coming soon
- Compatibility between high-end PCB standards and high-pin-density parts
- BJT moisture testing – how much does elevated moisture increase the risk of failure?
- Ceramic capacitor assurance
- Cubesat reliability
  - Inherited items process principles to cubesats and standard cubesat components

National Aeronautics and Space Administration

PCB assurance



SAFETY and MISSION ASSURANCE DIRECTORATE Code 300

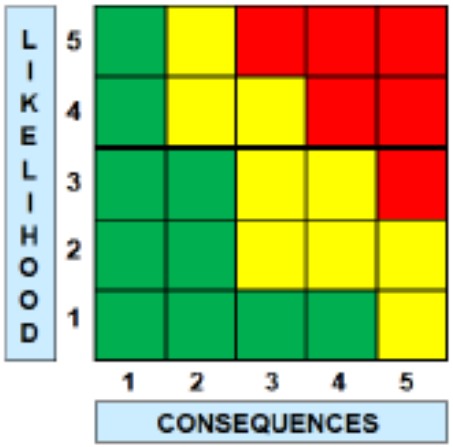
25

SMA SAFETY and MISSION ASSURANCE NASA Goddard

www.nasa.gov

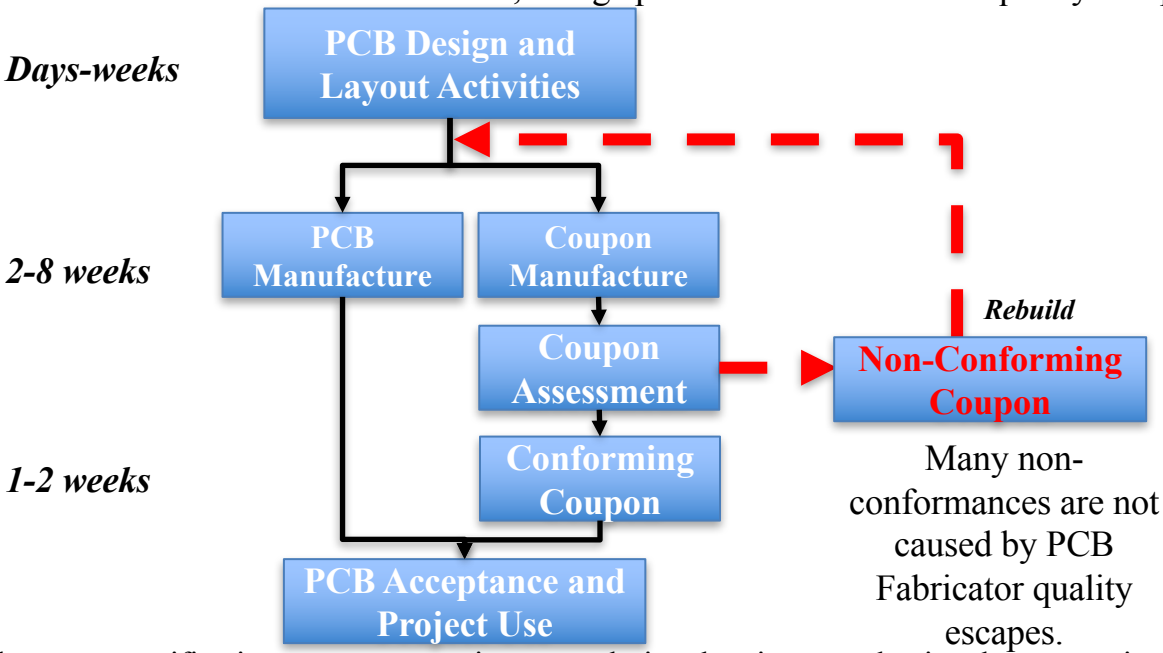
Impact of Non-conformances

- Bare boards cost $$ and build schedules – expensive!!
- But failures are even more expensive!
- Test sample nonconformance is not the same as PCB failure.
- Risk-based decisions are used for disposition of non-conformances.
- Non-conformances may have little to no impact per application.
- Began to explore origins and merit of requirements (more later).



PCB Assurance – Historical Approach

We see a general 20-30% rate of non-conformance, a large portion is not a result of quality escapes.

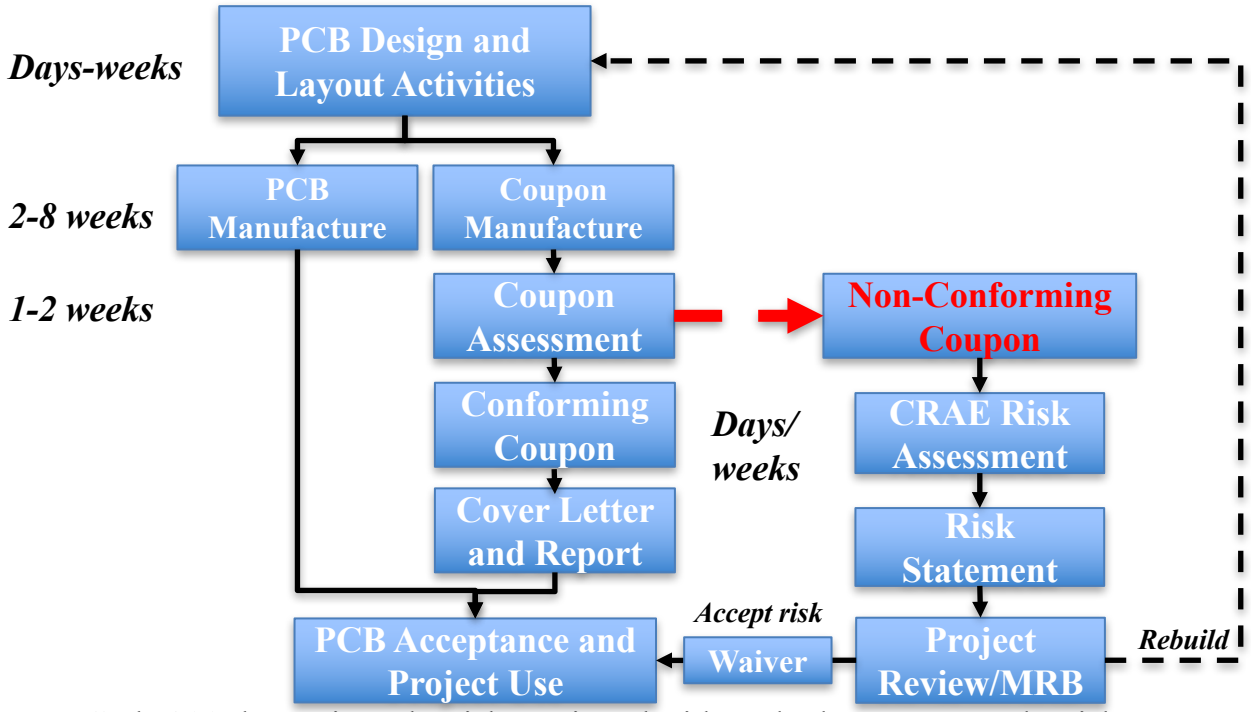


Inconsistencies between specifications, contract requirements, design drawings, production documentation, and coupon inspection lab submittals. Requirements were ambiguous. Voluntary consensus Standard requirements were interpreted conservatively, without a basis in risk.

Risk Assessment

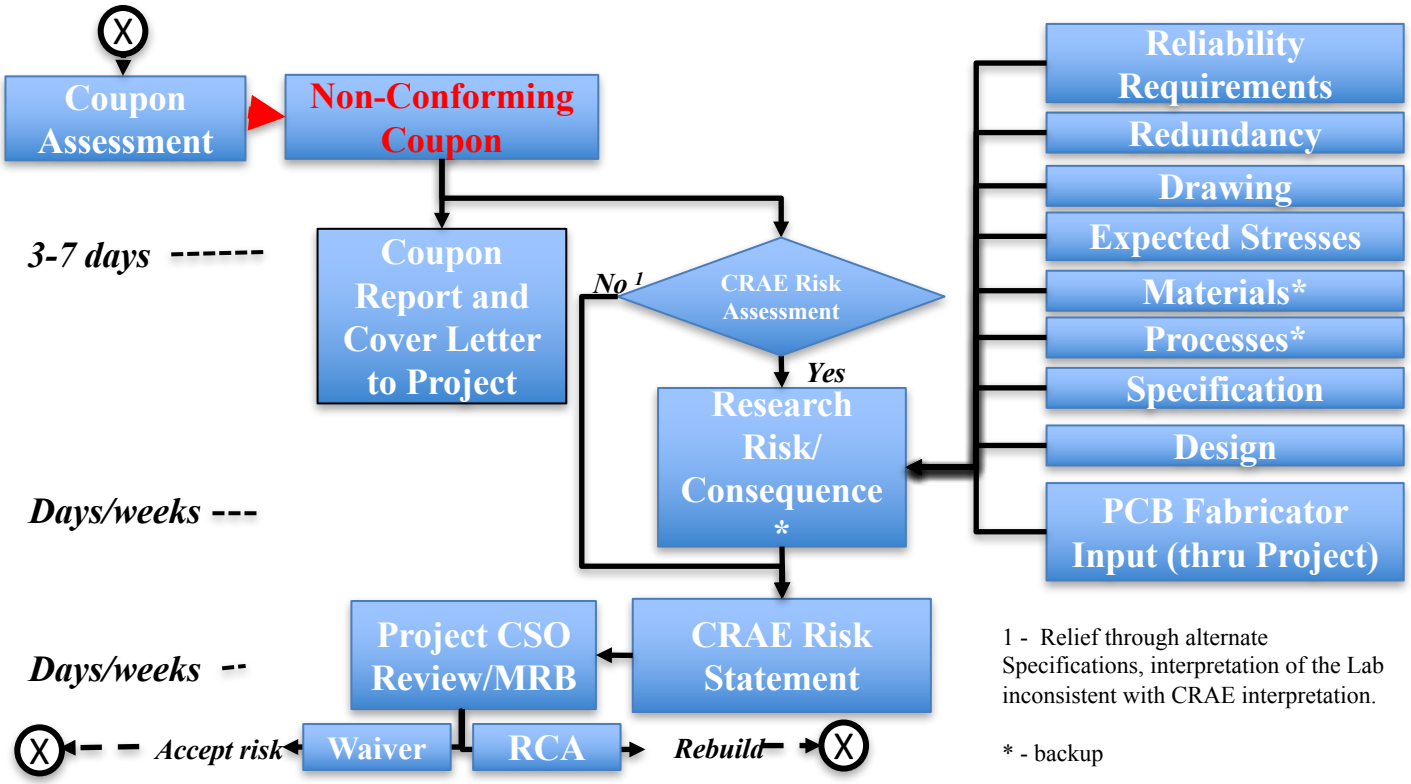
- Traceable PCB test coupons (designed per specs. such as IPC-2221B) are submitted to GSFC or to a GSFC-assessed laboratory.
- Reports that indicate nonconformance are dispositioned by risk assessment performed prior to refabricating or populating the PCB.
  - If risk assessment indicates elevated risk due to the nonconformance, then use is dispositioned by MRB.
- More than 170 PCB lots assessed for risk since 2014, > 85% dispositioned as UAI, significant cost and schedule savings.
  - $M's in cost savings, 100's of weeks of schedule savings over 3 years
- Risk assessment process eliminates waste and saves money and schedule, lowers overall risk for the project.
- The process reduces the need for repeated attempts to refabricate.

PCB Assurance – Current Approach



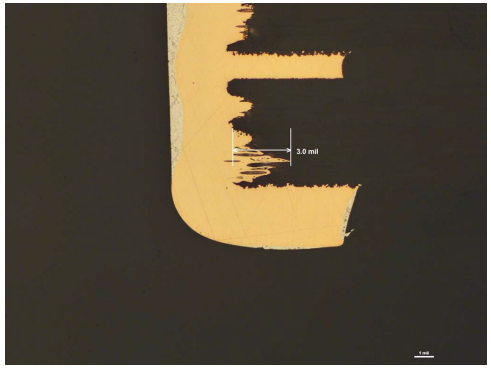
Code 300 determines the risk, project decides whether to accept the risk.

Risk Assessment Approach



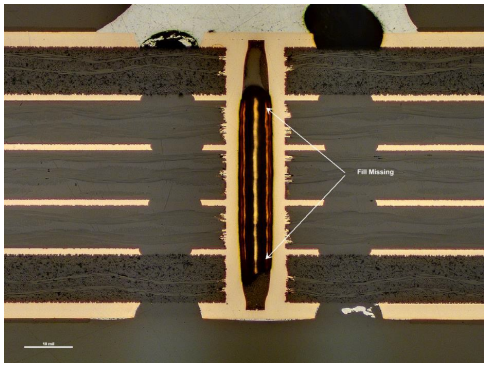
Sampling of Risk Assessments – 1

Copper wicking in excess of 2.0 mil



The wicking is well-enclosed within the annular rings with significant margin, and should not violate electrical spacing. When inspected with IPC-6012 DS, these boards would be compliant (max 3.5 mil wicking + etchback).

Capped via with fill less than 75%



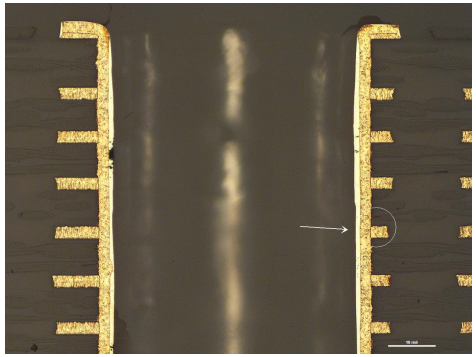
Voiding is contained and enclosed within the fill material (with matches in CTE with the PCB laminate), and does not appear to have an interface with the cap where contaminants could potentially trap.

Sampling of Risk Assessments – 2

Dielectric layer less than 3.0 mil

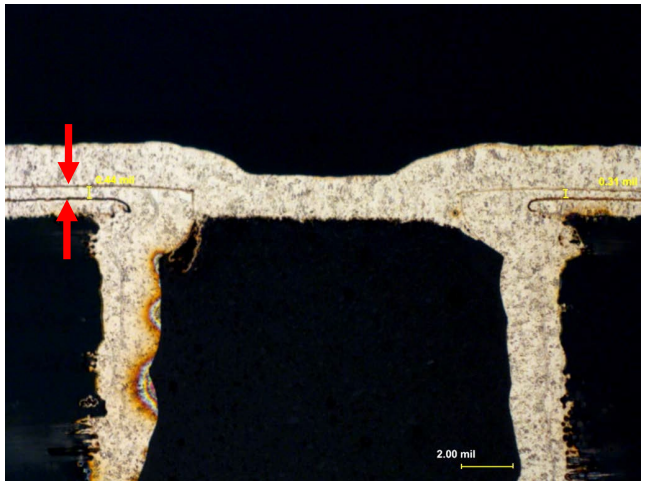
A 40kV dielectric breakdown strength, combined with a 28V service voltage provides a sufficient dielectric clearance at 2.8mil. There are at least two layers of dielectric material present.

IAR less than the minimum 5.0 mil



Out of date drawing notes containing a minimum 5.0mil annular ring and other requirements.

PTH Copper Wrap Thickness Requirement



- Thermal cycle stresses act on interfaces, outer layers experience the greatest stress.
- Reason: materials selection and geometry.

Per IPC-6012D for through-holes:

Class 1	AABUS
Class 2	5 µm [197 µin]
Class 3 & 3/A	12 µm [472 µin]

AABUS = As Agreed Between User and Supplier

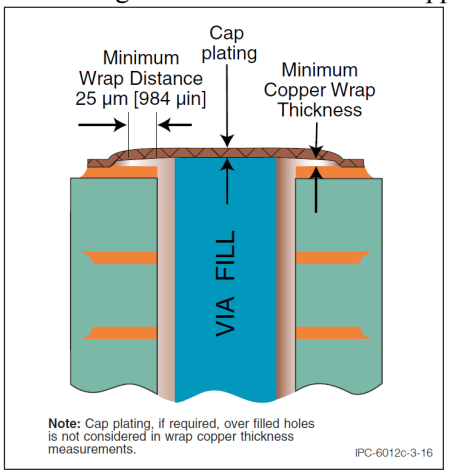


Figure 3-16 Surface Copper Wrap Measurement (Applicable to all filled PTHs)

*reference IPC 6012D standard © IPC

PTH Copper Wrap Thickness: Disposition

- A GSFC mission had a populated and integrated board with zero wrap; wrap planarization can cause 0.3mil or more variance in panel; manufacturers must target more wrap.
  - Wrap cannot be achieved at required thickness for designs with tight line-width spacing and/or with multiple lamination/plating steps
- Requirement was introduced to IPC with minimal data
  - Reliability reported to be better with wrap vs. butt joint
  - Half of barrel plating thought to be "good enough"
  - Higher quality limit used as safety margin against manufacturing variation during planarization
- **GSFC Studies:** Determined the impact of copper wrap plating thickness on PCB reliability, as characterized by thermal cycles to failure.
  - Able to determine acceptability of wrap defect based on reliability testing and analysis in context of mission environment and duration.
  - IPC voted to change the requirement (amendment in Rev. D and revisions in Rev. E).

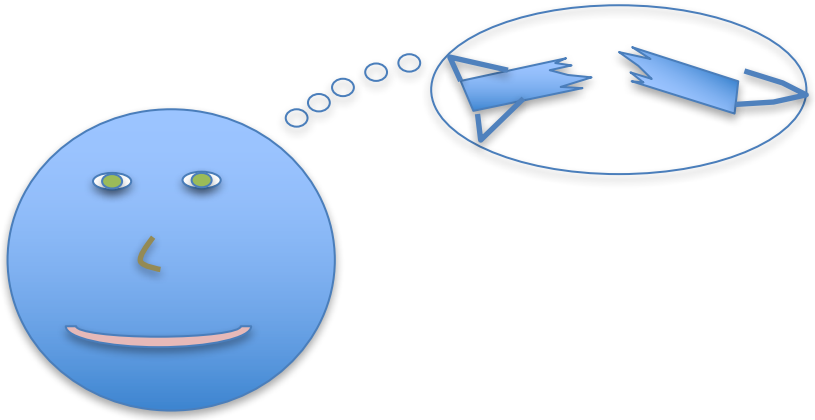
Summary

We talked about:

- Risk Classification and Risk-based SMA
- Day in the life
- Risk-based audit and assessment
- Risk-based SMA examples and current activities
- PCB process example

Backup materials

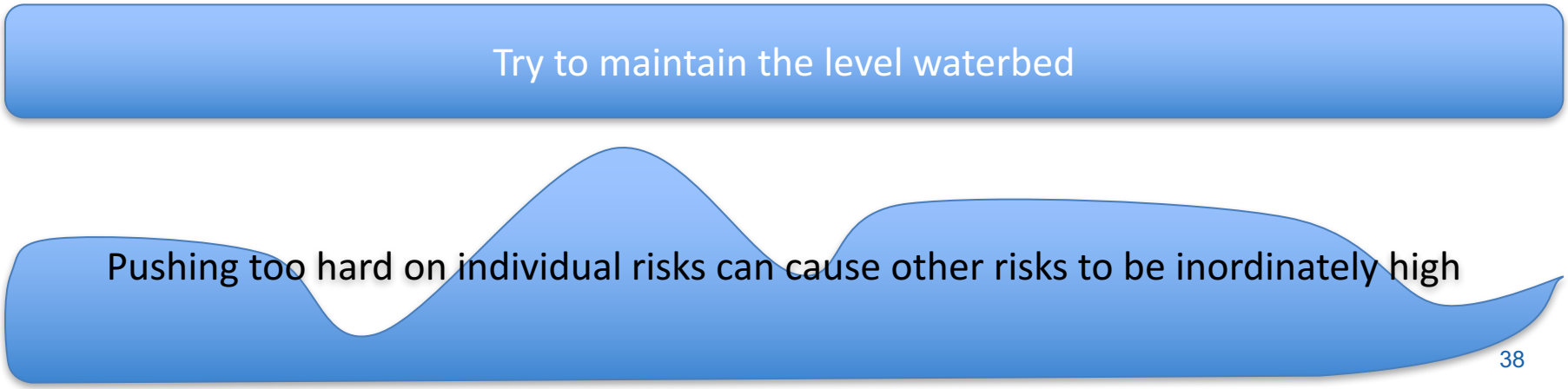
Risk vs Possibility



- Failure modes and mechanisms can appear through
  - Analysis and simulation
  - Observation
  - Prior experiences
  - Brainstorming “what if” scenarios
  - Speculation
- These all constitute *possibilities*
- There is a tendency to take action to eliminate the possibilities of severe consequences
- When a possibility is combined with an environment, an operating regime, and supporting data, a risk can be established – this is core to the engineering process
- Too much attention to eliminate possibilities can lead to excessive cost and unbalanced risk

Balanced Risk (maintaining a level waterbed)

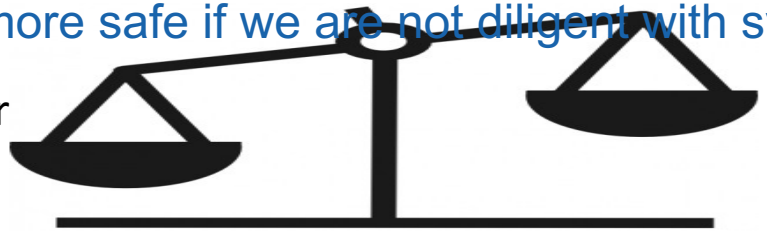
- A systems approach of looking across all options to ensure that mitigating or eliminating a particular risk does not cause much greater risk somewhere in the system



Unbalanced Risk Example

- General safety requirements dictate that anything considered "safety" requires 3 inhibits.
- Unfortunately, many elements prior to launch vehicle separation that are tied solely to mission success are put under the safety umbrella.
- This means that by default, many items such as premature deployment of solar arrays or other appendages are considered a safety issue for the on-orbit portion, even if they have no range safety effect, and they prompt a decision that it is always better to have more inhibits even if such a design prompts an even greater risk of mission failure due to one of the inhibits not releasing.
- Ultimately, under the guise of “safety” we may end up with a less reliable system that is not more safe if we are not diligent with system-level thinking

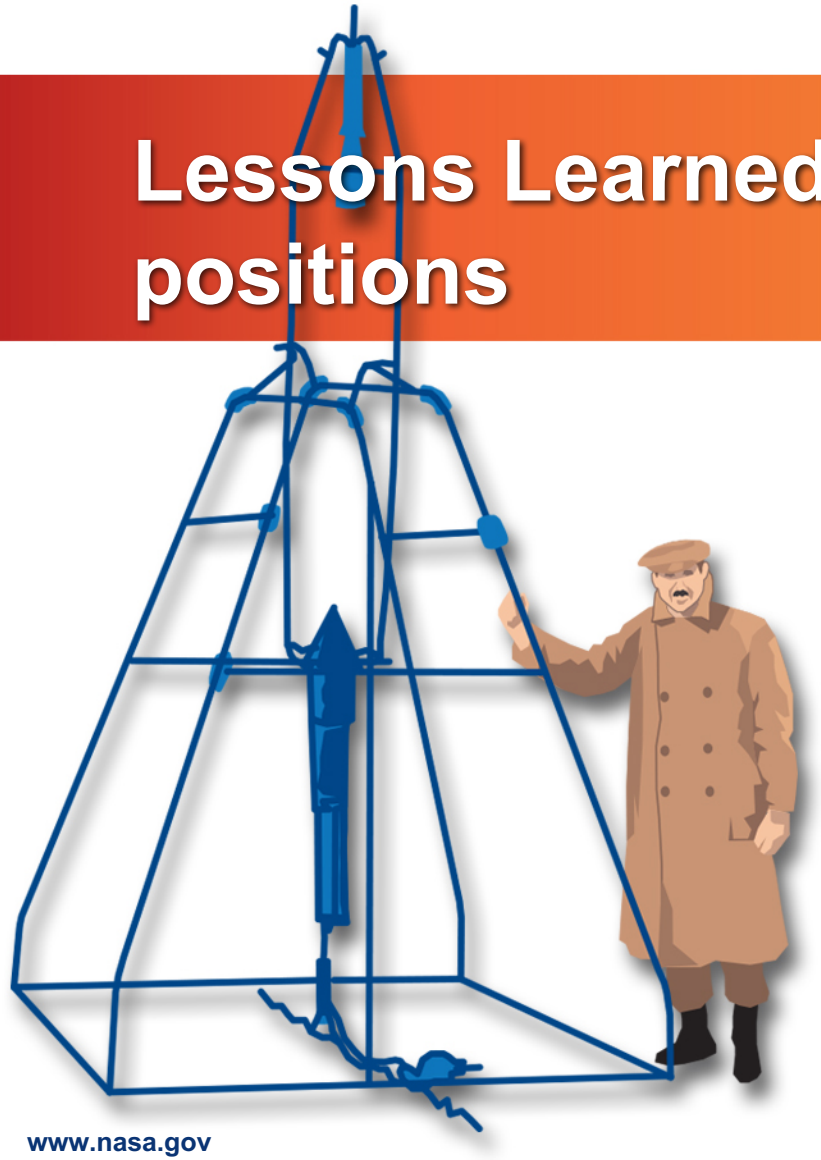
Reliability under the safety umbrella



Reliability not under the safety umbrella

National Aeronautics and Space Administration

Lessons Learned and the new positions



SAFETY and MISSION ASSURANCE DIRECTORATE Code 300

SMA SAFETY and MISSION ASSURANCE NASA Goddard

What problems are we solving?

- We unnecessarily repeat many things
- Lessons learned are not conveyed at all the right levels
- Lessons learned are not conveyed in an effective way
- Requirements do not appropriately account for our experiences
- We tend to do things because we've always done them
- Lessons learned are not considered in everyday practices
- Red herrings are running amok

Events to learn from

- Analyses performed
- Technical assessments
- Risk Assessments
- Failures
- Anomalies
- Mishaps
- Close calls
- Project conflicts
- Procurements
- Nonconformances and dispositions
- Cost overruns
- Schedule problems

Existing lessons learned artifacts

- SMA top ten
- Watchlist
- GIDEPs, NASA advisories, and MWARs
- SMA CE wiki

Handling Concepts, new and old

- Day-to-day responsibility within key positions
- Requirements evaluation board
  - Testing for reqmts evaluation
  - Requirements changes
- Close call monthly or quarterly briefing
- Wiki communication and discussion
- Code 300 risk board, 400 risk advisory board
- MSR briefings
- Alert mechanisms
  - Watchlist
  - GIDEP
  - NASA advisory
- Entry into lessons learned system

People

- MPAEs
- PRAEs
- CRAEs
- QEs
- REs
- Auditors

Introduction to the new positions

- CRAE: Commodity Risk Assessment Engineer
- PRAE: Parts and Radiation Assurance Engineer
- MPAE: Materials and Processes Assurance Engineer

PRAE (373)
(Assigned directly to multiple projects)

- Ensure EEE parts requirements and guidelines reflect experiences
- Ensure that risk is the primary driver for parts-related decisions
- Ensure that parts entering the parts control board are prioritized by risk
  - Focus on high risk parts/high risk applications
  - Minimize efforts on low risk parts/applications
- Establish cross-cutting dispositions and processes for EEE parts-related alerts and advisories
- Maintain database of parts experiences
- Establish acceptability/risk of vendor parts practices

MPAE (373)
(Assigned directly to multiple projects)

- Ensure materials and processes requirements and guidelines reflect experiences
- Ensure that risk is the primary driver for materials-related decisions and acceptance/denial of material usage
- Ensure that materials approvals are prioritized by risk
  - Focus on high risk materials/high risk applications
  - Minimize efforts on low risk materials/applications
- Establish cross-cutting dispositions and processes for materials-related alerts and advisories
- Maintain database of materials experiences, e.g., where process problems cause major project issues
- Establish acceptability/risk of vendor materials practices

Specifics

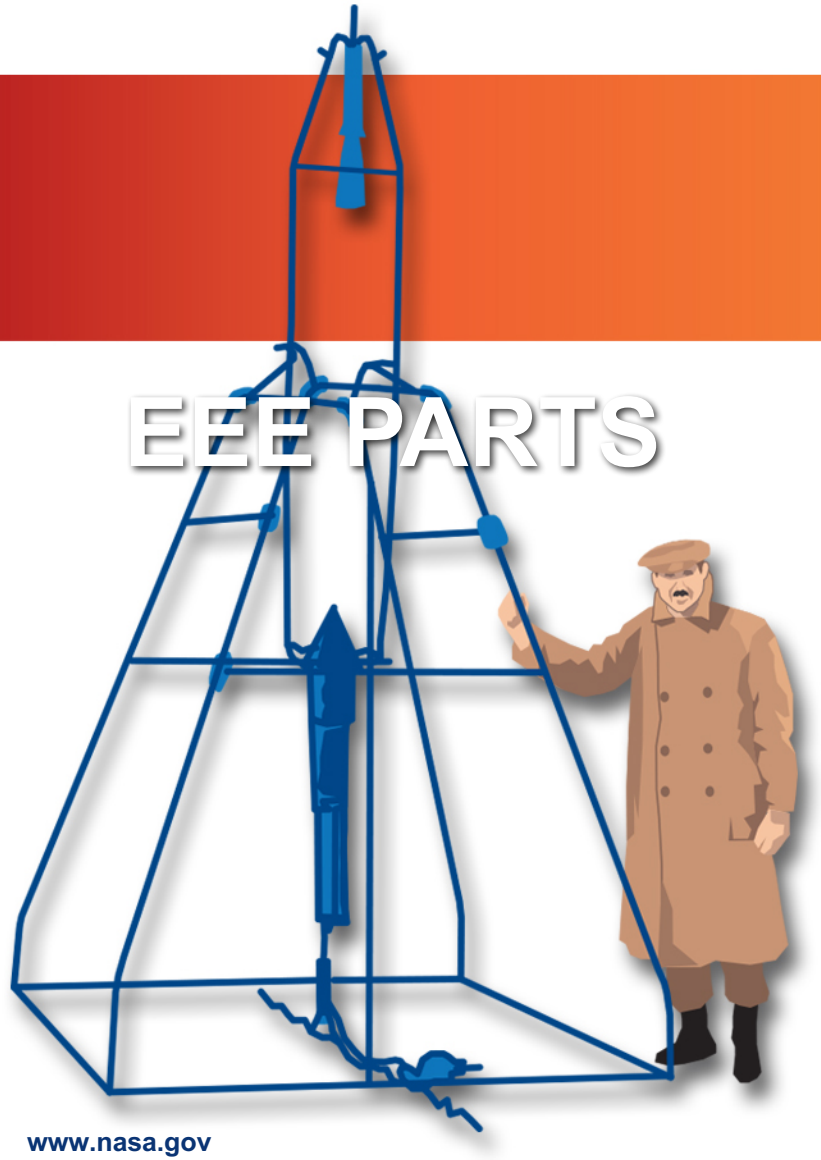
- Review all parts and materials lists
- Invited to all PCBs, MPCBs, etc. (not voting)
- Review or drive agendas for PCBs, MPCBs, MUA disposition
- Reach-out to vendors
- Review parts and materials related alerts for applicability and cross-cutting disposition
- Put parts and materials related decisions in project risk context
- Perform risk assessments when decisions cause problems in project or with vendors
- Document all issues encountered and risk assessments
- Ensure that vendor nonconformances and notable observations get to supply chain managers
- Act as a cross-cutting set of eyes
- Head off problems caused by requirements overreach and creep
- Focus overly broad prohibitions into proper context (e.g., press-fit connectors, RNC 90 resistors, table II and III materials, etc)
- Understand common vendor practices at all vendors

CRAE (371)
Senior Technical positions in 300

Commodity: Tangible or intangible entity that has a major impact on risk, cost or schedule for GSFC projects

- Expert in key discipline area with background and experience with reliability and risk
  - Responsible and empowered to assign risks based on warnings, alerts, environments, and "what we are stuck with"
    - Establishes testing programs and protocols to keep up with current design practices and common parts and components
      - Sets the policies for the risk-based decisions on use of parts, components, and processes
        - Establishes layers of risk reduction based on risk classification (ownership of GPR 8705.4)
          - Determines the acceptability and risk of alternate standards or requirements, or deviations and non-conformances
            - Answers, *"are we ok?" "why are we ok?" "how ok are we?"*
              - Provides risk assessment to the project for the project to decide how they want to disposition

National Aeronautics and Space Administration



EEE PARTS

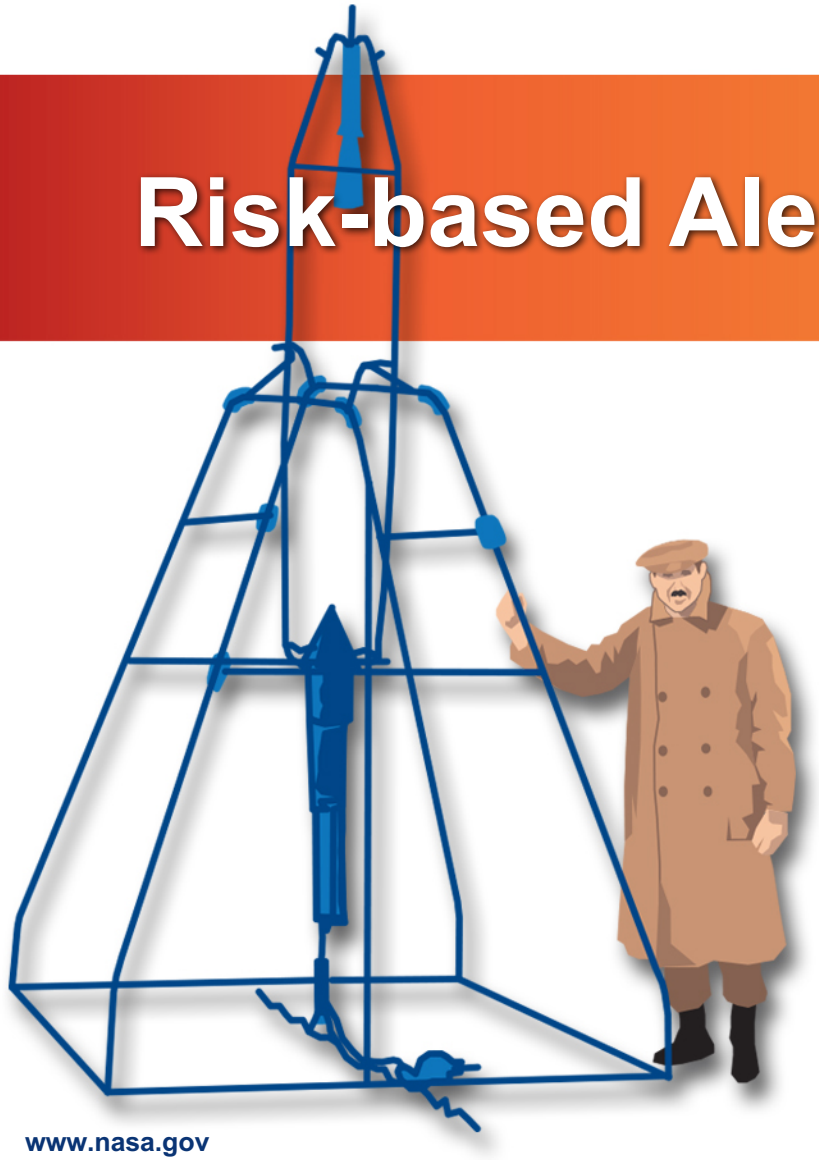
SAFETY and MISSION ASSURANCE DIRECTORATE Code 300

SMA SAFETY and MISSION ASSURANCE NASA Goddard

www.nasa.gov

National Aeronautics and Space Administration

Risk-based Alert handling



SAFETY and MISSION ASSURANCE DIRECTORATE Code 300

SMA SAFETY and MISSION ASSURANCE NASA Goddard

Advisories

- Defined
  - Statements warning of problems experienced in the broad community
- Examples
  - GIDEP alert
  - GIDEP problem advisory
  - NASA advisory
  - Agency Action Notice
  - External warning (from MDA, Aerospace, etc)
  - Code 300 watchlist item
- Generally not written with “ease of closure” in mind
- Generally introduces “possibility” of a problem and the challenge is to get to “risk”

GSFC's historical approach to closure

- GIDEP alerts and advisories, NASA advisories, and AANs sent out to all projects after careful review of applicability from GIDEP coordinator/representative
- Projects individually need to prove
  - Beyond a reasonable doubt they are unaffected
    - Some include having to provide closeout photos
  - All affected stakeholders within the project understand the risk when there is an impact
- When projects have a direct hit
  - Provide all lot date codes
  - Answer 6 detailed questions
  - Get sign off from MSE, CSO, PDL in the project for use
  - Even if (1) there is no risk, (2) the questions are not relevant, (3) the lot date codes are not relevant
- Based on "verify", not on "trust"

What can make an advisory hard to close?

- Ubiquitous part (2N2222, CWR06, etc)
- Noncompliance to a lesser-used parameter in a spec
- Parts are installed
- Parts in a component purchased from a sub
- Difficulty in tracing the entire supply chain
- Lack of root cause for problem
- Complex technical details to describe the concern
- Problem sounds bad but may not pose risk to us at all in our context

Unintended Consequences

- Without careful thought and context in providing the warning, we can drive up risk
  - Semicoa laser hole
  - Micropac 53250
  - Crane converters
  - Transistor moisture
- A huge amount of resources can go to buy down very low risk
  - Vishay resistors
  - Semicoa laser hole
  - VisionTech Counterfeit parts
- There is a propensity to feel like you have to “do something” about a product that has a warning, before it is determined that there is risk in its use

Example: Semicoa laser-etching hole GIDEP

- Encountered on MMS
- The nonconformance is a combination of having a laser hole that penetrates all the way into the part and falsely passing the leak tests
- Failure requires presence or corrosive agent, pressure to have it enter the hole, and other conditions to cause corrosion
- Problem has existed in some form since at least as far back as 2004.
- Over time parts were collected from across the electronics community (ultimately ~1M) and we were seeing about 12 ppm exhibiting the nonconformance defined above.
- 10 ppm is an approximate threshold for JANS part failures where red flags are raised, so 12 ppm just for the nonconformance would result in a failure rate much lower => this problem does not cause an abnormally high failure rate

Semicoa GIDEP cont'd

- Responding to this GIDEP was painful and costly for projects with many of these parts (ubiquitous part)
- Responding to this GIDEP drove up risk for several projects
  - Boards were pulled from boxes that had gone through environmental test, packaged up, shipped to GSFC, and inspected
  - Without intervention, some boards that had already gone through rework were going to be reworked
  - It is likely many risky events occurred that we were not aware of.
- It took almost a year of effort and a very detailed rigorous reliability assessment to prove that the potential for failure was well within that expected for MIL-SPEC parts.

The intent is often misinterpreted

- Some developers wait until parts are installed in hardware before responding, instead of using the warnings preventatively
- Some will pull parts out of hardware without a basis in risk, or they will ignore the risk of pulling the parts
- Some believe that when we ask to assess the risk of use-as-is, that there is always elevated risk.
- Advisory are sometimes meant only to be advisory

How do we transition to risk-based?

- Review all advisories in a cross-cutting sense before providing to projects
  - Gather SME inputs
  - Determine if there is likely risk to GSFC projects
  - Make all efforts to disposition at the Center level
- In “stuck with” situations, ensure that risk is captured for all options
- Do not demand information that is not necessary to assess the risk
- Create two bins
  - Those that require approval from management based on proof
    - Where efforts to disposition are commensurate with risk-level
  - Those that report to management if the problem affects them
    - Where efforts to disposition are likely far greater than the risk-level

Cross-cutting disposition approach

- SME reviews advisory in the following attributes
  - Is the advisory descriptive enough to provide clear applicability and direction for GSFC projects?
  - Is the advisory overcome by GSFC's normal practices?
  - Does the advisory represent a completed analysis (e.g., is there any question whether a part actually failed or if the author killed the part)?
- SME evaluates potential risks vs resources required
- SME works to identify broad recommendations
- SME works with projects individually as needed
- If project-specific tasks are left, then project will complete the closure

Goal of dispositioning advisories

- When possible use advisories preventively to avoid problems when procuring
- Eliminate or mitigate risks associated with advisories
- Avoid increasing risk in projects through unintended consequences
- Properly document closure